



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/731,371	12/09/2003	Hong-Hsi Lo	ORACL-01416US1	4427
80548	7590	02/18/2010		
FLIESLER MEYER LLP 650 CALIFORNIA STREET 14TH FLOOR SAN FRANCISCO, CA 94108				
EXAMINER				
WANG, HARRIS C				
ART UNIT		PAPER NUMBER		
2439				
NOTIFICATION DATE		DELIVERY MODE		
02/18/2010		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

OFFICEACTIONS@FDML.COM

Office Action Summary

Application No.

10/731,371

Applicant(s)

LO ET AL.

Examiner

HARRIS C. WANG

Art Unit

2439

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 November 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 3, 7-14, 16, 20-25 and 52-62 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 3, 7-14, 16, 20-25, 52-62 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ ~~Notice of Informal Patent Application~~
- 6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

Applicant argues that "in Fichtner there does not appear to be any interaction in the authentication process between the different backend HTTP servers to be signed on"

There does not appear to be any claim limitations requiring the backend servers to interact.

The Applicant further argues "in Fichtner, the authentication server...is centralized and separate from the various backend HTTP servers (pg. 12 of Remarks)."

This is consistent with the Examiner's interpretation of the "first" and "second" server, where the CAP (or authentication server) is the first server and the backend server is the second.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3, 7-14, 16, 20-25, 52-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher (20030033535) in view of Fichtner (20030005297).

Regarding Claims 1,13, 60

A system for single security administration comprising:

A first application server of a first server type, which is configured to execute transaction processes including receiving calls from clients to initiate the transaction processes, wherein the first application server includes

a LDAP authentication server plugin which is configured to forward the calls from clients to another application server for authorization;

("Fig. 2 shows a block diagram illustrating the architecture 200 of an exemplary common authentication protocol or proxy (CAP) server 40 according to one embodiment of the invention" Paragraph [0019]). The Examiner interprets the CAP server as the first authentication server. The Examiner interprets the "first type server" as the CAP server in conjunction with the plurality of Applications that may call it

a second application server of a second server type, which is configured to administer security for the first application server, wherein the second application server includes *("The architecture of the Cap server includes...an authentication interface which communicates with directory service backends including...LDAP" Paragraph [0019])* The Examiner interprets the authentication backend the second server.

a user profile database which includes security information for a plurality of users, including for each of the users a mapping of security credentials for that user between the first server type and the second server type,

("the CAP server will perform authentication by accessing the database of the appropriate authentication backend for the given application...it obtains the user or user group information it requires to perform authentication function from an external user or user group database contained in an authentication backend" Paragraph [0023]) The Examiner interprets the data repository as the database. The Examiner interprets the user security information as the authentication or credential information.

an embedded LDAP server which is configured to receive the calls from the LDAP authentication server plugin;

wherein, when a call is received from a client to initiate a transition at the first application server , the LDAP authentication server plugin

identifies the user associated with the call

determines that the second application server should authenticate the user

Initiates an LDAP session between the first application server and the second application server

Sends a query information to the embedded LDAP server

receives from the embedded LDAP server a corresponding user

information as determined by the user profile database at the second application server

creates a token, reflecting the result, which is subsequently used to authenticate the client to participate in the transaction

("A user 30 wishes to begin an application 20 on the data processing system...The application 20 will send a request for authentication credentials 300 to the CAP server 40 (step 420) Paragraph [0021]) The Examiner interprets the application as the default security plugin that receives authentication requests from clients and forwards them to an authentication server. ("Secure Channel from the Client...Security is provided by encapsulation at the transport layer so that alternate security methods may be used or "plugged in." Paragraph [0123]) *("The invention addresses the need to reduce user logon complexity at the desktop while offering the open architecture to integrate easily into current enterprise environments...CAP...allows applications to access existing directory service authentication backends" Paragraphs [0006-0007]) ("If the credentials are authentic, then the CAP server will return an authentication token to the application." Paragraph [0024])*

Fisher does not explicitly teach wherein the first type server holds only access control list which defines user security information

Fichtner (2003/0005297) teaches wherein a first type server holds the access control list (ACL) and relies on one of the plurality of second type servers to provide user and group information *("Then based on each...backend server's sign-on credentials for each user or group, the administrator may...map application user identity to the backend HTTP server identity" Paragraph [0054]) ("The authentication server of the application then checks the requested Web Resource's ACL policy against the internal credential of the user to verify if access is allowed for the user" Paragraph [0056])* Therefore Fichtner teaches the

authentication server holding the access control list and relying on the backend servers to provide group and user information.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Fisher to include keeping the ACL at the first server and the group and user information at the second server.

The claim would have been obvious because a particular known technique (keeping the ACL in one server and user and group information in a second server) was recognized as part of the ordinary capabilities of one skilled in the art.

Regarding Claims 3, 16

Fisher and Fichtner teach the system of claim 1. Fisher teaches wherein the first server is an enterprise server (See Figure 1, Application **20** and CAP **40**.) Fisher teaches wherein said second server is an application server (*"This architecture supports and takes advantage of existing enterprise user/group authentication backends 110"* Paragraph [0126] of Fisher).

As the first server serves the needs of an enterprise it is considered an enterprise server.

Regarding Claim 7, 20

Fisher and Fichtner teach the system of claim 1 wherein said query information is query user information that specifies a particular user or group of users. (*"In general, the CAP server...obtains the user or user group information it requires to perform its authentication function from an external user or user group database contained in the authentication backend"* Paragraph [0023])(LDAP User Filter, LDAP Group Filter, Paragraph [0095-6] of Fisher)

Regarding Claim 8, 21

Fisher and Fichtner teach the system of claim 1 wherein the system includes a plurality of servers

(*"The invention seeks to provide a method and system for user authentication in a data processing system wherein users only have to logon once, while being able to access multiple applications and servers"* Paragraph [0006] Fisher)

Regarding Claim 9, 22

Fisher and Fichtner teach the system of claim 8 wherein at least one of said plurality of servers include an LDAP authentication server. (*"LDAP Server Host"* Paragraph [00941])

Fisher does not explicitly teach where at least two servers include an LDAP authentication server.

It would have been obvious to one of ordinary skill in the art at the time of the invention to include two LDAP authentication servers.

The motivation is that Fisher already teaches using multiple servers, including one LDAP server. The mere duplication of parts does not produce any unexpected results. One of ordinary skill in the art would have been able to add another LDAP server without altering the functionality of the system.

Regarding Claim 10, 23,

Fisher and Fichtner teach the system of claim 1, further comprising a user information cache that caches a copy of said user information. (*"the authentication token is generally stored in cache memory within the data processing system and is passed to each application that the user needs to access without the need to request new credentials each time"* Paragraph [0030]) The Examiner interprets the authentication token as comprising use credentials.

Regarding Claim 11, 24

Fisher and Fichtner teach the system of claim 1. The Examiner asserts that any system which has multiple servers and is compatible with LDAP (including the system of Fisher) is scalable to include multiple LDAP authentication servers and/or multiple embedded LDAP servers.

Regarding Claim 12, 25,

Fisher and Fichtner teach the system of claim 1 wherein at least one of said servers include a console program for administering the security of the system. (*"The CAP server includes an administration system that provides a system administrator with the ability to change or configure the CAP server's properties. Configuration may be HTML based. The HTML page may be generated by a servlet. The administration screens may be accessible from a browser, and editor, or an enterprise information portal."* Paragraph [0084]) The Examiner asserts that an administration system as described inherently requires a computer program.

Regarding Claim 52,

Fisher and Fichtner teach the system of claim 1 wherein:

The session is a LDAP session that supports a single user security data store and administration (*Figure 1, "LDAP"*)

Regarding Claim 54,

Fisher and Fichtner teach of claim 1, wherein:

The first type server also supports a separate independent authentication mechanism with a separate security repository (*Figure 2 shows multiple separate authentication mechanisms*)

Regarding Claim 55,

Fisher and Fichtner teach of claim 53, further comprising:

A migrating utility that takes user security information from the separate security repository associated with the first type server and updates the security data repository associated with at least one of the plurality of second type servers. (*Paragraph [0041] see the "import" operation*)

Regarding Claim 53, 56, 58, 62

Fisher and Fichtner teach the system of claim 1 wherein:

Fisher and Fichtner do not explicitly teach each of the plurality of second type of servers supports backup or failover authentication

The Examiner takes Official Notice that backup or failover authentication is well known.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the servers support backup or failover authentication.

The motivation is to provide support in case communication fails.

Regarding Claims 57, 59, 61

Fisher and Fichtner teach the system of claim 1.

Fisher and Fichtner do not explicitly teach wherein the first type server is Tuxedo-based and the second type is not Tuxedo based.

The Examiner takes Official Notice that Tuxedo is a well known type of server.

It would have been obvious to one of ordinary skill in the art to use a Tuxedo based server for the first server and a non-Tuxedo based server for the second.

The use of the Tuxedo type server does not alter the way the system functions in any way and one of ordinary skill would know that the inclusion of a Tuxedo server would provide predictable results.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARRIS C. WANG whose telephone number is (571)270-1462. The examiner can normally be reached on M-F 9-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, EDAN ORGAD can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Harris C Wang/
Examiner, Art Unit 2439

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439